Claims

1. In a method of enforcing geographical restrictions on content redistribution in a TCP/IP network, an improvement comprising defining a geographical boundary across which certain content does not pass, wherein said boundary is defined – at least in part –

5   by a hardware firewall device.

2. The method of claim 1 that includes determining whether an IP packet should be regarded as conveying content that should not cross said boundary, by reference to flag bits included in the header of said packet.

10

3. The method of claim 2 wherein said flag bits are related to the payload of a watermark in the content.

4. In a method of data processing that includes forming an IP packet having

15   header data and body data, wherein the header data includes a first destination address, an improvement comprising forming said header data to additionally include additional data specifying whether it is permissible to send a copy of data in the packet to a second destination address.

20   5. The method of claim 4 wherein the additional data has at least two states, respectively indicating:

(a) it is not permissible to send a copy of data in the packet to any second destination address; or

(b) it is not permissible to send a copy of data in the packet to any second

25   destination address except to a second destination address within a domain that also includes the first destination address.

6. The method of claim 5 wherein said domain comprises networked devices associated with a single family.

30

7. The method of claim 4 wherein a device associated with the first destination address has a first physical location and a device associated with the second destination address has a second physical location, and the additional data includes a field signaling that copying of data in said packet to said second destination address should be:

5   (a) permitted if the second physical location is physically proximate to the first physical location; and

(b) prohibited if the second physical location is physically remote from the first physical location.

10   8. The method of claim 7 wherein the first and second destination addresses are within a common domain.

9. The method of claim 7 wherein the first and second destination addresses both correspond to network devices associated with a single family.

15

10. The method of claim 4 wherein said additional data is related to the payload of a watermark encoded in the body data.

11. In a method of data processing that includes receiving an IP packet having

20   header data and body data, wherein the header data includes a first destination address, the first destination address corresponding to a device at a first physical location proximate to where said method is practiced, an improvement comprising interpreting additional data in the header of said packet as specifying whether it is permissible to send a copy of data in the packet to a second destination address.

25

12. The method of claim 11 wherein:

(a) if the additional data has a first state, prohibiting transmission of a copy of data in the packet to any second destination address; and

(b) if the additional data has a second state, prohibiting transmission of a copy of

30   data in the packet to any second destination address other than a second destination address within a domain that also includes the first destination address.

13. The method of claim 12, wherein said domain comprises networked devices associated with a single family.

5   14. The method of claim 11 wherein a device associated with the second destination address has a second physical location and wherein:

(a) if the second physical location is physically proximate to the first physical location, permitting copying of data in said packet to the second destination address; and

(b) if the second physical location is physically remote from the first physical location, prohibiting copying of data in said packet to the second destination address.

10

15. The method of claim 14 wherein the first and second destination addresses are within a common domain.

15   16. The method of claim 14 wherein the first and second destination addresses both correspond to network devices associated with a single family.

17. The method of claim 14 wherein the method includes determining whether the second physical location is physically remote from the first physically location by

20   reference to whether the second destination address is served by a common firewall with the first destination address.

18. The method of claim 11 wherein said additional data is related to the payload of a watermark encoded in the body data.

25

19. A method wherein content is divided and collectively represented by plural packets of data, each packet having first and second portions, the first portion of each packet including a divided part of the content, the method including obtaining an identifier of said content, and including said content identifier in the second portion of

30   each packet.

20. The method of claim 19 wherein said obtaining includes examining a previous representation of said content that has an identifier associated therewith.

5   21. The method of claim 19 wherein the packets comprise IP packets, each having a body portion as said first portion, and a header portion as said second portion, said header portion including address information in addition to said content identifier.

22. The method of claim 19 wherein the packets comprise non-contiguous blocks

10   of data in a storage medium, said blocks being associated together by a table of file allocation data.

23. The method of claim 22 wherein each of said non-contiguous blocks includes a content identifier, but data in said table does not.

15

24. The method of claim 19 that further includes reading the content identifier from the second portion of one of said packets to identify content represented by data in the first portion.

20